ACTA ARITHMETICA
LXXXIV.2 (1998)

On some polynomials allegedly related to the *abc* conjecture

by

Alexandr Borisov (University Park, Penn.)

1. Introduction. The main goal of this paper is to call your attention to the following family of polynomials.

Definition 1.1. For every $a = b + c$, where a, b, c are coprime natural numbers the *abc-polynomial* is defined to be

$$f_{abc}(x) = \frac{bx^a - ax^b + c}{(x-1)^2}.$$

I discovered these polynomials when pursuing a rather naive approach to the Masser–Oesterlé's *abc* conjecture. The following argument describes the idea.

Argument. Although the arithmetic *abc* conjecture is a great mystery, its algebraic counterpart is a rather easy theorem. It looks like it was first noticed by W. W. Stothers (cf. [19]). Later on it was generalized and rediscovered independently by several people, including R. C. Mason (cf. [11]) and J. Silverman (cf. [17]).

Theorem. *Suppose $a + b + c = 0$, where a, b, c are coprime, not all constant, polynomials with coefficients in a field K with* $\operatorname{char} K = 0$. *Suppose $R(x) \in K[x]$ is the product of all irreducible monic polynomials from $K[x]$ that divide abc. Then*

$$\deg R \geq \max(\deg a, \deg b, \deg c) + 1.$$

There are several proofs of this theorem, all involving derivatives or differential forms. I will discuss two of them, probably the easiest ones, and then try to translate them into the arithmetical setting.

1991 *Mathematics Subject Classification*: Primary 11R09; Secondary 12A20, 14G99.

The easiest proof, due to Oesterlé (cf. [13]) is to differentiate the equality $a(x)+b(x)+c(x)=0$ and consider the Wrońskian

$$D=\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}=\begin{vmatrix} b & c \\ b' & c' \end{vmatrix}=\begin{vmatrix} c & a \\ c' & a' \end{vmatrix}.$$

The theorem is then obtained by comparison of the degree of D and the powers in which primes dividing abc divide D.

The second proof (the original proof of Stothers [19], cf. also Mason [11], Silverman [17]) is to consider the map $\varphi : P^1 \to P^1$ given by $a(x)/c(x)$ and apply the Hurwitz ramification formula.

Both of the above proofs are hard to follow in the arithmetic case. The reason is that there is no such map φ and no non-zero differentiation. This is related to the fact that the set of integers is naturally discrete so they do not have any non-trivial deformations. However, the integers have "quantum" deformations: for any positive integer a, one defines $[a]_q = q^{a-1}+\ldots+q+1$ where q is a quantum parameter. Other people call this a q-expansion. The classical integers are obtained by specializing q to 1.

Let us try therefore to "quantize" the abc conjecture. In order to deal with positive integers we rewrite $a+b+c=0$ as $a=b+c$, with a, b, c positive, possibly switching a, b, and c and changing some signs. The equality $a=b+c$ can then be quantized as $[a]_q=[b]_q+[c]_q q^b$.

Another way to go is $[a]_q=[b]_q q^c+[c]_q$. They yield basically the same. Unfortunately, the extra q-factor cannot be avoided.

Following the first proof, consider

$$D=\frac{1}{q-1}\begin{vmatrix} b & a \\ [b]_q & [a]_q \end{vmatrix}=\frac{b(q^a-1)-a(q^b-1)}{(q-1)^2}=\frac{bq^a-aq^b+c}{(q-1)^2}.$$

It naturally corresponds to the D in Oesterlé's proof. Note now that this is exactly the abc-polynomial $f_{abc}(q)$.

This abc-polynomial also arises if one tries to follow Stothers' proof as a non-trivial factor of the derivative of $[a]_q/[c]_q$:

$$\left(\frac{[a]_q}{[c]_q}\right)'=\frac{q^{c-1}}{[c]_q^2}\left(\frac{bq^a-aq^b+c}{(q-1)^2}\right).$$

So this is how these polynomials appear. The exact comparison with the geometric case is definitely lost at this point. However, the abc-polynomials do have some really nice properties.

First of all, it looks like they are always irreducible. This question is naturally invariant under the switch of b and c because $f_{abc}(x)$ is reciprocal to $f_{acb}(x)$. In the case when it is irreducible, it is natural to call the corresponding field the *abc-field*. It only depends on the triple $a=b+c$ and not on the order of b and c. It has degree $a-2$ and is unramified outside of

abc, which follows from the direct calculation of the discriminant of $f_{abc}(x)$ (Lemma 2.1).

Although the author has no knowledge of any previous investigations on *abc*-polynomials in the general case, the particular case $c = 1$ (or $b = 1$) was studied before. First of all, Nicolas and Schinzel studied the distribution of roots of

$$f_{n,1,n-1}(x) = \frac{x^n - nx + (n-1)}{(x-1)^2}$$

in the complex plane and obtained some remarkably precise results on it (cf. [12]).

Also, M. Filaseta conjectured that $f_{n+1,n,1}(x) = (x^n + x^{n-1} + \ldots + x + 1)'$ is always irreducible. He proved it for n being a prime power (cf. Theorem 3.1). T. Y. Lam conjectured that all the higher derivatives $(x^n + x^{n-1} + \ldots + x + 1)^{(k)}$ are also irreducible. Using the methods of this paper (with some significant modifications) for any fixed k one can prove the irreducibility for almost all (in the sense of density) n. These results will appear elsewhere in a joint paper with Filaseta and Lam. In this paper we prove that $f_{abc}(x)$ are irreducible for the density one set of coprime triples ($a = b + c$). We also prove the same result for any fixed b. And for "good" b, that is, if there is a prime p such that $p \,\|\, b$, we prove that all but finitely many *abc*-polynomials are irreducible. To be more precise, it suffices to assume that $c \gg b \ln b$.

The irreducibility results of this paper can be viewed as part of a more general problem of irreducibility of the kernels of trinomials. It was extensively studied by Schinzel (cf. [14]). From the older results on this topic I should mention that of Selmer (cf. [16]).

The paper is organized as follows. Section 2 contains the results about the distribution of roots of *abc*-polynomials in the usual and p-adic complex numbers. The key Section 3 is devoted to the irreducibility results which rely heavily on the results of Section 2. Section 4 contains some miscellaneous remarks and heuristics that I have gathered in the unsuccessful attempt to link the *abc*-polynomials closer to the *abc* conjecture from which they originated.

A more detailed version of this paper, which in particular more fully explains the author's motivation for studying the *abc*-polynomials, is currently available in the Algebraic Number Theory Archives

(http://www.math.uiuc.edu/Algebraic-Number-Theory/)

or directly from the author.

Notations. Throughout the paper, if we write $g(x) \mid f_{abc}(x)$ we assume that $g \in \mathbb{Z}[x]$ and $f_{abc}(x)/g(x) \in \mathbb{Z}[x]$. All signs $\gg$ and $\ll$ assume absolute constants unless specified otherwise. The notation $m \,\|\, n$ means, as usual, that $m \mid n$ and $\gcd(m, n/m) = 1$.

Acknowledgments. I am taking this opportunity to thank my Penn State adviser Yuri Zarhin for his interest and support of this research in its embryonic stage. I also thank A. Schinzel for the reference to Filaseta and Lam's work. I am especially thankful to M. Filaseta whose numerous helpful comments and interest in this study helped me push it a lot farther than what I originally thought possible. In particular, Lemma 3.1 for $k > 1$ and the current version of Theorem 3.7 are due to him. The crucial part of this research was conducted while at the University of Georgia whose hospitality is thankfully acknowledged.

2. Distribution of roots. First of all, let us calculate the discriminant of the *abc*-polynomial.

LEMMA 2.1. *The discriminant of $f_{abc}(x)$ is equal to $2a^{a-3}b^{a-4}c^{a-4}$.*

Proof. First of all, $f_{abc}(1) = \frac{1}{2}(bx^a - ax^b + c)''(1) = abc/2$. Denote by (u, v) the resultant of the polynomials u and v. Then the discriminant of $f_{abc}(x)$ is calculated as follows:

$$\begin{aligned}
\frac{1}{b}(f, f') &= \frac{1}{b}\left(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)(x-1) - 2(bx^a - ax^b + c)}{(x-1)^3}\right) \\
&= \frac{1}{b}\left(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)(x-1) - 2(bx^a - ax^b + c)}{(x-1)^2}\right)\frac{2}{abc} \\
&= \frac{1}{b}\left(\frac{bx^a - ax^b + c}{(x-1)^2}, \frac{abx^{b-1}(x^c-1)}{x-1}\right)\frac{2}{abc} \\
&= \frac{2}{a^2c}\left(\frac{b(x^c-1)x^b - c(x^b-1)}{(x-1)^2}, \frac{x^c-1}{x-1}\right)c^{b-1}(ab)^{a-2} \\
&= \frac{2}{ab^2c}c^{b-1}(ab)^{a-2}\left(\frac{b(x^c-1)x^b}{x-1} - c\frac{x^b-1}{x-1}, \frac{x^c-1}{x-1}\right)\frac{1}{c} \\
&= 2a^{a-3}b^{a-4}c^{b-3}\left(c\frac{x^b-1}{x-1}, \frac{x^c-1}{x-1}\right) \\
&= 2a^{a-3}b^{a-4}c^{b-3}c^{c-1} = 2a^{a-3}b^{a-3}c^{a-4}.
\end{aligned}$$

REMARK 2.1. The Mahler measure M of $f_{abc}(x)$ is at most $2a$, which can be shown by applying Mahler's result [9] to the corresponding trinomial. Therefore Mahler's estimate for the discriminant (cf. [10]) implies that $D(f_{abc}(x)) \le (a-2)^{a-2}(2a)^{2a-6}$ which is of about the same magnitude as the exact value, especially if b is about the same as c. This means that the roots are more or less uniformly distributed around the unit circle. In Theorem 2.1 we make it much more precise using the result of P. Erdős and P. Turán (cf. [4]).

Let us prove now that $f_{abc}(x)$ is the kernel of the corresponding trinomial (i.e. it has no roots on the unit circle).

LEMMA 2.2. (1) *If* $bx^a - ax^b + c = 0$ *and* $|x| = 1$, *then* $x = 1$.
(2) $f_{abc}(1) = abc/2$.
(3) $f_{abc}(x)$ *is coprime to its reciprocal* $f_{acb}(x)$.

Proof. (1) If $|x| = 1$ then $|bx^a| = b$, $|ax^b| = a$, $|c| = c$. So in order for x to be the root the above three numbers have to lie on the same ray. So x^b and x^a have to be 1. This implies that $x = 1$ because $\gcd(a, b) = 1$.

(2) We actually proved it at the beginning of the proof of Lemma 2.1.

(3) If $f_{abc}(x) = f_{acb}(x) = 0$ then

$$a\left(\frac{x^b - 1}{x - 1} \cdot \frac{x^c - 1}{x - 1}\right) = f_{abc}(x) + f_{acb}(x) = 0,$$

which is impossible by (1).

LEMMA 2.3. *For* $a = b + c$, *coprime*, $f_{abc}(x)$ *has exactly* $b - 1$ *roots inside and* $c - 1$ *outside the unit circle.*

Proof. Instead of $f_{abc}(x)$ it is easier to consider the trinomial $bx^a - ax^b + c$ itself. It has, besides the roots of $f_{abc}(x)$, a double root at 1. If we deform c by a very small *negative* real number, $-\varepsilon$, then the polynomial $g_\varepsilon(x) = bx^a - ax^b + (c - \varepsilon)$ will have simple roots close to the roots of $f_{abc}(x)$ as well as two simple real roots near 1, one smaller and one greater than 1. This follows from the fact that

$$bx^a - ax^b + c - \varepsilon = -\varepsilon + \frac{abc}{2}(x - 1)^2 + O(x - 1)^3$$

as $x \to 1$. As a result, for ε small enough the number of roots of $g_\varepsilon(x)$ inside the unit circle is exactly one plus the number of roots of $f_{abc}(x)$ in there. Notice now that if $|x| = 1$, then

$$|ax^b| = a = b + c > b + c - \varepsilon = |bx^a| + |c - \varepsilon| \geq |bx^a + c - \varepsilon|.$$

So, when x makes one revolution around 0 on the unit circle, ax^b makes b revolutions and so does $g_\varepsilon(x)$.

Therefore, $g_\varepsilon(x)$ has b roots inside the unit circle, and $f_{abc}(x)$ has $b - 1$. The remaining $c - 1$ roots of $f_{abc}(x)$ are outside the unit circle.

LEMMA 2.4. *If* a *is even then* $f_{abc}(x)$ *has no real roots. If* a *is odd it has exactly one real root which is always negative.*

Proof. If a is even, then b and c are odd (since a, b, and c are pairwise coprime) and Descartes' Rule of Signs implies that the polynomial $bx^a - ax^b + c$ has at most and, hence, exactly two positive real roots corresponding to the two roots at 1, and no negative real roots. Similarly, if a is odd, then Descartes' Rule of Signs implies that $bx^a - ax^b + c$ has the two positive

roots at 1 and no other positive roots and exactly one negative real root. The lemma follows.

The following lemma is a trivial observation that will be needed in Theorem 3.7.

LEMMA 2.5. *If $a \geq 4$ then for every root $x = re^{i\varphi}$ of $f_{abc}(x)$ we have $r = |x| < 2$.*

Proof. First of all, if $f_{abc}(x) = 0$ then

$$x^c = \frac{a}{b} - \frac{c}{bx^b}.$$

If $r > 1$ then

$$r^c \leq \frac{a}{b} + \frac{c}{b} = 1 + \frac{2c}{b}.$$

If $c < b$ then we estimate $r < 1 + 2/b$, as

$$\left(1 + \frac{2}{b}\right)^c = 1 + \frac{2c}{b} + R,$$

where the remainder term R is obviously positive. In this case, because $b > a/2$, $r < 1 + 4/a \leq 2$.

If $c > b$, then we estimate

$$r \leq \left(1 + \frac{2c}{b}\right)^{1/c} \leq (2c+1)^{1/c} < 2$$

because $c \geq 3$ for $a \geq 4$.

LEMMA 2.6. *For every $\varepsilon > 0$ there exists some positive constant $A(\varepsilon)$ such that for every $x = re^{i\varphi}$ which is a root of $f_{abc}(x)$, its absolute value r satisfies the inequality*

$$|r - 1| < (1 + \varepsilon)\frac{2}{a}\ln(2a) \quad \text{if } a \geq A(\varepsilon).$$

Proof. It is clearly enough to prove the upper bound due to the symmetry of the problem. We proceed as in the previous lemma, so we get

$$r \leq \left(1 + \frac{2c}{b}\right)^{1/c}.$$

If $c < b$ the bound is even better than what we need.

If $c > b$, then $r \leq (1 + 2c/b)^{1/c}$ implies

$$\ln r \leq \frac{1}{c}\ln\left(1 + \frac{2c}{b}\right) \leq \frac{1}{c}\ln(2c+1).$$

So if $c \gg 1$ ("$\gg$" depends on ε) we have

$$r < 1 + \left(1 + \frac{\varepsilon}{3}\right)\frac{1}{c}\ln(2c+1) < 1 + \left(1 + \frac{\varepsilon}{2}\right)\frac{1}{c}\ln(2c).$$

So if $a \gg 1$ ("$\gg$" depends on ε) then

$$r < 1 + (1+\varepsilon)\frac{2}{a}\ln(2a),$$

which proves the lemma.

The following result is due to P. Erdős and P. Turán.

THEOREM (P. Erdős–P. Turán, [4]). *Suppose the roots of the polynomial* $f(x) = a_n x^n + \ldots + a_1 x + a_0$ *are denoted by* $x_k = r_k e^{i\varphi_k}$, $k = 1, \ldots, n$. *For every* $0 \le \varphi \le \psi \le 2\pi$ *denote by* $N_f(\varphi, \psi)$ *the number of* x_k *such that* $\varphi \le \varphi_k \le \psi$. *Then*

$$\left| N_f(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n \right| < 16\sqrt{n \ln \frac{|a_0| + |a_1| + \ldots + |a_n|}{\sqrt{|a_0 a_n|}}}.$$

REMARK 2.2. Instead of the Erdős–Turán theorem one can also use a somewhat similar result of Bilu ([1]), which in the case of *abc*-polynomials gives a little bit worse and ineffective bound.

Now we apply the above theorem to $f_{abc}(x)$.

THEOREM 2.1. *In the above notations for any* φ, ψ,

$$\left| N_{f_{abc}}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n \right| \le 12\sqrt{n\ln(n+1)},$$

where $n = a - 2 = \deg f_{abc}(x)$.

P r o o f. By the Erdős–Turán theorem applied to $bx^a - ax^b + c$ we have

$$\left| N_{f_{abc}}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}n \right| \le \left| N_{bx^a - ax^b + c}(\varphi,\psi) - \frac{\psi-\varphi}{2\pi}(n+2) \right| + 2$$

$$< 16\sqrt{n \ln \frac{2a}{\sqrt{a-1}}} + 2.$$

One can easily check that, say, for $n \ge 100$,

$$16\sqrt{n \ln \frac{2a}{\sqrt{a-1}}} + 2 < 12\sqrt{n\ln(n+1)}$$

when $a = n + 2$. And for $n < 100$ the theorem is true anyway because $12\sqrt{n\ln(n+1)} > n$.

REMARK 2.3. In the case $b = 1$ there is a much more precise result of Nicolas and Schinzel (cf. [12]). It would be very interesting to extend it to the general case.

Consider now the distribution of roots of $f_{abc}(x)$ in the p-adic complex fields for $p \mid abc$. First of all, we decompose $f_{abc}(x)$ modulo primes that divide either a, b, or c.

LEMMA 2.7. (1) *For every* $p \mid a$,

$$f_{abc}(x) \equiv b\left(\frac{x^{a_1}-1}{x-1}\right)^q (x-1)^{q-2} \bmod p,$$

where $q = p^k$ *is the maximum power of* p *dividing* a *and* $a_1 = a/q$.

(2) *For every* $p \mid b$,

$$f_{abc}(x) \equiv -c\left(\frac{x^{b_1}-1}{x-1}\right)^q (x-1)^{q-2} \bmod p,$$

where, similar to above, $q = p^k$, $b = qb_1$, $(b_1, p) = 1$.

(3) *For every* $p \mid c$,

$$f_{abc}(x) \equiv bx^b\left(\frac{x^{c_1}-1}{x-1}\right)^q (x-1)^{q-2} \bmod p,$$

where $q = p^k$, $c = qc_1$, $(c_1, p) = 1$.

Proof. The proofs of all three statements are straightforward. Let us prove just one of them, say (3). The $A \equiv B$ below means that $A - B = pU(x)$, where $U(x)$ is a rational function with integer coefficients and monic denominator. We have

$$\begin{aligned} f_{abc}(x) &= \frac{bx^a - ax^b + c}{(x-1)^2} \equiv \frac{bx^a - ax^b}{(x-1)^2} \equiv bx^b \frac{x^c - 1}{(x-1)^2} \\ &= bx^b \frac{x^{c_1 q} - 1}{x^q - 1} \cdot \frac{x^q - 1}{(x-1)^2} \equiv bx^b \left(\frac{x^{c_1}-1}{x-1}\right)^q (x-1)^{q-2}. \end{aligned}$$

This proves the desired formula.

Because of the above decomposition, it is very natural to consider the roots in the p-adic complex field as coming in clusters around the a_1th (or b_1th, c_1th) roots of unity and 0 (for $p \mid c$) and ∞ (for $p \mid b$). The p-adic distance between the above roots of unity is obviously equal to 1, so the clusters do not have common roots.

LEMMA 2.8. *Suppose that* $p \mid a$, $a = qa_1$, $(p, a_1) = 1$, $q = p^k$. *Suppose we fix a* p*-adic complex field with valuation* v, $v(p) = 1$. *Then for every* $\zeta \neq 1$, $\zeta^{a_1} = 1$, *we have exactly* p *roots* x_i *of* $f_{abc}(x)$ *with* $v(x_i - \zeta) = 1/p$, *exactly* $p^2 - p$ *roots with* $v(x_i - \zeta) = 1/(p^2 - p)$, *exactly* $p^3 - p^2$ *roots with* $v(x_i - \zeta) = 1/(p^3 - p^2)$, *and so on, until exactly* $p^k - p^{k-1}$ *roots with* $v(x_i - \zeta) = 1/(p^k - p^{k-1})$.

Proof. The roots of $f_{abc}(x)$ that are inside the unit ball with center $\zeta \neq 1$, $\zeta^{a_1} = 1$, are the roots of $bx^a - ax^b + c$, because $v(\zeta - 1) = 0$. Consider the polynomial $g(x) = b(\zeta + x)^a - a(\zeta + x)^b + c$. Its roots are exactly the

differences between roots of $f_{abc}(x)$ and ζ. We have

$$g(x) = (b\zeta^a - a\zeta^b + c) + \sum_{j=1}^{a} x^j \left[b\binom{a}{j}\zeta^{a-j} - a\binom{b}{j}\zeta^{b-j} \right].$$

So

$$g(x) = a(1-\zeta^b) + \sum_{j=1}^{a} x^j \left[b\binom{a}{j}\zeta^{a-j} - a\binom{b}{j}\zeta^{b-j} \right].$$

So, if $g(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_a x^a$, then $v(u_0) = k$. For $1 \le j \le a$ if $v(u_j) < k$ or $v\big(\binom{a}{j}\big) < k$ then $v(u_j) = v\big(\binom{a}{j}\big)$. It is standard and easy to check that

$$v\left(\binom{a}{j}\right) = v\left(\frac{a}{j}\right) \quad \text{for } 1 \le j \le p^k.$$

So, for any $0 \le n < k$ the least j such that $v(u_j) \le n$ is $j = p^{k-n}$.

Combined with the Newton polygon method (cf. N. Koblitz, [8], Chapter 4) this proves the lemma.

LEMMA 2.9. *Suppose $p \mid a$, $a = p^k a_1$, $(a_1, p) = 1$. Then there are exactly $p-2$ roots x_i of $f_{abc}(x)$ with $v(x_i - 1) = 1/(p-2)$ (no such roots if $p = 2$), also exactly $p^2 - p$ roots with $v(x_i - 1) = 1/(p^2 - p)$, ... exactly $p^k - p^{k-1}$ roots with $v(x_i - 1) = 1/(p^k - p^{k-1})$.*

P r o o f. Similar to the lemma above, consider

$$g(x) = f_{abc}(1+x) = \frac{b(1+x)^a - a(1+x)^b + c}{x^2} = \sum_{j=2}^{a} x^{j-2}\left[b\binom{a}{j} - a\binom{b}{j} \right].$$

If $g(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_{a-2} x^{a-2}$, then for $1 \le j \le p^k - 2$,

$$v(u_j) = v\left(b\binom{a}{j+2} \right) = v\left(\frac{a}{j+2} \right)$$

whenever at least one (consequently all) of the above three numbers is less than k.

Notice also that $v(u_0) = k$ if $p \ne 2$ and $v(u_0) = k - 1$ if $p = 2$.

The rest of the proof is absolutely similar to that of the above lemma.

LEMMA 2.10. *Suppose $p \mid c$, $c = p^k c_1$, $(c_1, p) = 1$. Then there are exactly b roots x_i of $f_{abc}(x)$ such that $v(x_i) = k/b$. The remaining $c-2$ roots are located in clusters around c_1th roots of unity, exactly as for $p \mid a$.*

P r o o f. When we look for x_i such that $v(x_i) > 0$ it is enough to consider $g(x) = bx^a - ax^b + c$.

We have $v(c) = k$, $v(a) = 0$, and the first statement follows easily from the Newton polygon method. The proof of the second one is completely parallel to the two lemmas above and is omitted for brevity.

Lemma 2.11. *Suppose* $p \mid b$, $b = p^k b_1$, $(b_1, p) = 1$. *Then there are exactly* c *roots with* $v(x_i) = -k/c$. *The remaining* $b-2$ *roots are located in the same way as for* $p \mid a$.

Proof. Let us just recall that the roots of f_{abc} are reciprocal to the roots of f_{acb}. Then everything follows from the previous lemma.

3. Irreducibility results. We start with some relatively simple irreducibility results and proceed gradually to the harder and stronger ones.

Theorem 3.1. *Suppose* $c = 1$ *and* $b = p^k$, *where* p *is a prime. Then* $f_{abc}(x)$ *is irreducible.*

Proof. In the p-adic complex plane there is just one root x_i of $f_{abc}(x)$ with $v(x) < 0$. For all the rest $v(x) = 0$. So if $f_{abc}(x) = g_1(x)g_2(x)$ then one of g_i, say g_1, has leading coefficient ± 1. But this is impossible as all the roots lie strictly inside the unit circle (Lemma 2.3).

Remark 3.1. This result is due to M. Filaseta. Together with the first part of the next theorem it is probably all that was known about the irreducibility of *abc*-polynomials prior to this paper.

Theorem 3.2. *For any* $a = b+c$, *coprime*, $f_{abc}(x)$ *is irreducible if* $a = p$ *or* $a = 2p$, *where* p *is an odd prime.*

Proof. If $a = p$ then $f_{abc}(1 + x)$ is Eisenstein, so we are left with the case $a = 2p$. In the p-adic complex plane, we have p roots x_i of $f_{abc}(x)$ with $v(x_i + 1) = 1/p$ and $p - 2$ roots x_i of $f_{abc}(x)$ with $v(x_i - 1) = 1/(p - 2)$. If $f(x) = g(x)h(x)$ then, obviously, one of the polynomials g, h has to contain all roots from one cluster and one has to contain all roots from another one. This implies that, say, $\deg g = p, \deg h = p - 2$, a contradiction by Lemma 2.4.

Theorem 3.3. *For any* $a = b + c$, *coprime*, *the abc-polynomial is irreducible if* $a = pl$, *where* p *and* l *are distinct primes and the order of* p *in* $(\mathbb{Z}/l\mathbb{Z})^*$ *does not divide the number* N, *which is the integer from* 1 *to* l *defined by the property* $N \equiv (-2/p) \bmod l$.

Proof. Consider the roots of $f_{abc}(x)$ in the p-adic complex field. They come in clusters around lth roots of unity ζ_l. If $\zeta_l \neq 1$ then there are exactly p roots around it, at equal distance, $v(x_i - \zeta) = 1/p$. If $f_{abc}(x) = g(x)h(x)$ and g, h are with integer coefficients, then $v(g(\zeta_l))$ is an integer, because p is unramified in $\mathbb{Z}(\zeta_l)$. Therefore if g contains one root from the cluster of ζ_l it contains all of them. The same is true if $\zeta_l = 1$. Therefore, either $\deg g \equiv 0 \bmod p$ and $\deg h \equiv -2 \bmod p$, or the other way around. The same is obviously true for l instead of p.

As $\deg g$ and $\deg h$ are both less than $a-2$, we can assume that

$$\deg g \equiv 0 \bmod p, \qquad \deg g \equiv -2 \bmod l.$$

Therefore $\deg g = pN$, where N is the number from the statement of this theorem.

We can be a bit more precise. As $g(x)$ does not contain the roots around 1, and contains all or none of the roots from any of the clusters, its reduction modulo p has to be of the form $u(x)^p$, where $u(x)$ is some polynomial dividing $(x^l-1)/(x-1)$. But it is an elementary fact from the theory of cyclotomic fields that $(x^l-1)/(x-1)$ splits modulo p into the product of prime factors of the same degree k, where k is the order of p in $(\mathbb{Z}/l\mathbb{Z})^*$. As $\deg u = N$, k must divide N. But we assumed that it does not, so the theorem is proven.

REMARK 3.2. It looks like for most pairs (p,l) either (p,l) or (l,p) satisfies that extra condition from the above theorem. However, it is not the case, say, for $p=5$, $l=31$. So the above theorem is not applicable for $a=155$.

THEOREM 3.4. *If $c=2$, then $f_{abc}(x)$ is irreducible.*

P r o o f. By Lemma 2.10, in the 2-adic field we have b roots x_i of $f_{abc}(x)$ with $v_2(x_i) = 1/b$. So $f_{abc}(x)$ is irreducible (actually, Eisenstein).

THEOREM 3.5. *If $c=p$, p is odd prime, and a is even, then $f_{abc}(x)$ is irreducible.*

P r o o f. In the p-adic complex field we have b roots x_i of $f_{abc}(x)$ with $v_p(x_i) = 1/b$ and $p-2$ roots with $v_p(x_i-1) = 1/(p-2)$. So if $f_{abc}(x) = g(x)h(x)$ then $\deg g = b, \deg h = p-2$ or the other way around, contradiction by Lemma 2.4.

REMARK 3.3. The above theorems establish irreducibility for triples having density zero. The following theorem proves the irreducibility for a positive density set of triples abc.

THEOREM 3.6. *If b and c are both square-free and greater than 1, then $f_{abc}(x)$ is irreducible.*

P r o o f. By the obvious symmetry of the problem, we can assume that $b > c$. Then consider any prime $p \mid c$. In p-adic complex numbers there are exactly b roots of $f_{abc}(x)$ with p-adic valuation $1/b$. If $f(x) = g(x)h(x)$, $\deg g \geq \deg h$, then g has to contain all these roots. As this is true for any $p \mid c$, h has constant term ± 1.

Consider now any prime $p \mid b$. There are, again, exactly c roots of $f_{abc}(x)$ with p-adic valuation $-1/c$. Either g or h must contain them all. If this is h, then $\deg h \geq c$, which contradicts the equality $\deg g + \deg h = a-2$ $(< b+c)$. So, it is g again. As this is true for all $p \mid b$, $h(x)$ is monic. As $h(x)$ only contains roots with 0 p-adic valuations for all $p \mid bc$, we can apply the

argument of Theorem 3.3 to show that the residue of $\deg h(x)$ modulo any such p is 0 or -2. This implies that

$$bc \mid \deg h \cdot (\deg h + 2).$$

Therefore $\deg h \cdot (\deg h + 2) \geq bc > c^2$, so $\deg h > c - 2$. But this contradicts the fact that

$$\deg h(x) = a - 2 - \deg g(x) \leq a - 2 - b = c - 2.$$

REMARK 3.4. The above argument does not work in the case $c = 1$ as we have to have at least one prime dividing c to conclude that $\deg g(x) \geq b$.

Before going any further let us prove the following three lemmas.

LEMMA 3.1. *As always, we have $a = b + c$, coprime. Suppose $p \mid a$ (or $p \mid b$ or $p \mid c$) and $\zeta \neq 1$ is a non-trivial a_1th (or b_1th or c_1th) root of unity (in the notation of Lemmas* 2.8–2.11*). Consider its cluster of roots of $f_{abc}(x)$ in p-adic complex numbers. Suppose now that $g(x) \mid f_{abc}(x)$. Then the number of roots of $g(x)$ from the cluster of ζ is always divisible by p.*

Proof. We will consider the case $p \mid a$, because the same proof works in the other two cases as well. Suppose $a = p^k a_1$. It follows from the proof of Lemma 2.8 that the Newton polygon for $F(x) = f_{abc}(\zeta + x)$ has k non-horizontal edges of length p and $p^i(p-1)$, $i = 1, \ldots, k-1$, with slopes $1/p$ and $1/(p^i(p-1))$ respectively. Since the corresponding cyclotomic field is unramified at p, the Newton polygon for $G(x) = g(\zeta + x)$ has only integral vertices. Because $G(x) \mid F(x)$, all edges of G are edges or parts of edges of F. But there are no integral points inside the non-horizontal edges of the Newton polygon for F so the non-horizontal part of the Newton polygon for G consists of the whole edges of the one for F. Therefore the number of roots of $g(x)$ near ζ is a sum of some numbers from the set $\{p, p^i(p-1) : i = 1, \ldots, k-1\}$. All of them are divisible by p, which completes the proof of the lemma.

REMARK 3.5. One can also formulate and prove a similar result for the cluster of 1.

LEMMA 3.2. *Suppose $a = b + c$ is a coprime triple and $g(x) \mid f_{abc}(x)$. Then we have the following.*

(1) *If $p \parallel b$ (or, more generally, if $p^k \parallel b$, $\gcd(k, c) = 1$) then $g(x)$ contains all or no roots x_i of $f_{abc}(x)$ with $v_p(x_i) < 0$.*

(2) *If $p^k \parallel b$ and $\deg g(x) < c/\gcd(k, c)$ then $g(x)$ contains no roots x_i with $v_p(x_i) < 0$. As a result, if $\deg g(x) < c/\log_2 b$ then $g(x)$ is monic. (If $b = 1$ we treat $c/\log_2 b$ as $+\infty$, so the above condition is always satisfied.)*

Proof. If $p^k \parallel b$, $k \geq 1$, then there are c such roots x_i of $f_{abc}(x)$ with $v_p(x_i) = -k/c$. If N of them are the roots of $g(x)$ then $Nk/c \in \mathbb{Z}$. This

implies that in (1), N is 0 or c, and in (2), $N = 0$. The second conclusion in (2) is because $\gcd(k, c) \le k \le \log_2 b$.

LEMMA 3.3. *Suppose $g(x)$ is a polynomial with integral coefficients which divides $f_{abc}(x)$. Denote by A the following rational number associated with $g(x)$:*

$$A = \sum_{g(x_i)=0} (1 - x_i).$$

(a) *Suppose $p \mid a$. Then $p \mid A$ (i.e. $v_p(A) > 0$).*

(b) *Suppose $f_{abc}(x) = g(x)h(x)$, $p \parallel b$ (or, more generally, $p^k \parallel b$, $\gcd(k, c) = 1$). Then p always divides at least one of the two numbers $A(g)$ and $A(h)$.*

(c) *Suppose $f_{abc}(x) = g(x)h(x)$, $p \parallel c$ (or, more generally, $p^k \parallel c$, $\gcd(k, b) = 1$). Then p always divides at least one of $A(g)$ and $A(h)$.*

P r o o f. (a) By Lemma 3.1 the number of roots of $g(x)$ in every cluster of $\zeta \ne 1$ is divisible by p. Therefore

$$\begin{aligned} A_l &= \sum_{\zeta \ne 1} \sum_{\substack{g(x_i)=0 \\ v_p(x_i - \zeta) > 0}} (1 - x_i) x_i^l + \sum_{\substack{g(x_i)=0 \\ v_p(x_i - 1) > 0}} (1 - x_i) x_i^l \\ &\equiv \sum_{\zeta \ne 1} \#\{x_i : v_p(x_i - \zeta) > 0\} \cdot (1 - \zeta)\zeta^l \equiv 0, \end{aligned}$$

where $\alpha \equiv \beta$ means that $v_p(\alpha - \beta) > 0$.

(b) By Lemma 3.2 either $g(x)$ or $h(x)$ contains no roots x_i with $v_p(x_i) < 0$. So either $A_l(g)$ or $A_l(h)$ is divisible by p as in (a).

(c) Lemma 3.2 applied to $f_{acb}(x)$ and the reciprocals of $g(x)$ and $h(x)$ implies that either $g(x)$ or $h(x)$ contains no roots with $v_p(x) > 0$. The rest is as in (a).

THEOREM 3.7. *Suppose $b = 1$ and $a \ge 3$ is square-free. Then $f_{abc}(x) = f_{a,1,a-1}(x)$ is irreducible.*

P r o o f. Suppose $f(x) = g(x)h(x)$. Consider two numbers, $A = A(g)$ and $B = A(h)$. Because $b = 1$ they are both integers. By Lemma 3.3 and because a is square-free they are both divisible by a.

By Lemma 2.5 for every root x_i of $f_{abc}(x)$, $|x_i| < 2$. Therefore $\mathrm{Re}(x_i) < 2$, $\mathrm{Re}(1 - x_i) > -1$. So,

$$A = \sum_{g(x_i)=0} (1 - x_i) > -\deg g > -a$$

and the same for B. Since

$$A + B = A(f_{abc}(x)) = \sum_{bx_i^a - ax_i^b + c = 0} (1 - x_i) = a,$$

the only possibility (up to the switch of g and h) is that $A = a$, $B = 0$.

Because $b = 1$, for every prime $p \mid c$ we have just one root of $f_{abc}(x)$ in p-adic complex numbers with $v_p(x_i) > 0$. If $g(x)$ does not have it then as in the proof of Lemma 3.3(a) we have $p \mid A$. Because $A = a$ and $a \equiv 1 \bmod p$ we conclude that for every $p \mid c$, $g(x)$ has the corresponding root. But this implies that $h(x)$ does not have it, so the constant term of $h(x)$ is ± 1. This is impossible because by Lemma 2.3 all the roots of $f_{abc}(x)$ are outside the unit circle on the complex plane.

Remark 3.6. The above theorem proves irreducibility for a positive density set of a. I first proved it under the additional assumption that $c = a - 1$ is also square-free. By arguing as at the beginning of the next theorem, one can also prove that $f_{abc}(x)$ is irreducible if $b = 1$ and

$$\Big(\prod_{p|a} p\Big)^2 \prod_{p|a-1} p > 9a^2$$

with 9 being a really lazy constant.

One can also prove that the right hand side of the above inequality can be replaced by $C \cdot a \log^2 a$ where C is some small effective constant. This can be done by considering the sums of $x_i - 1/x_i$ instead of $1 - x_i$. This will be included in our joint paper with M. Filaseta and T. Y. Lam which is currently in preparation.

The remaining part of this paper is in fact motivated by this joint work. In particular, Theorem 3.10 and its Corollary may be viewed as generalizations of the special case $b = 1$ which was first obtained as part of this joint work.

Remark 3.7. The following theorem is our main result. It proves that $f_{abc}(x)$ is irreducible for the set of coprime triples having density one (which will be justified in Theorem 3.9).

Theorem 3.8. *Consider all coprime triples $a = b + c$, $b < c$. Then for every $\varepsilon > 0$ if a is large enough, and*

$$\Big(\prod_{p|a} p\Big)^2 \Big(\prod_{p\|b} p\Big)\Big(\prod_{p\|c} p\Big) > (4+\varepsilon)a^2 b \tag{1}$$

then $f_{abc}(x)$ is irreducible.

Proof. We will assume in the proof that $\varepsilon < 1$. Suppose $f_{abc}(x) = g(x)h(x)$. Consider $A = A(g)$ and $B = A(h)$ (in the notation of Lemma 3.3). Then if the leading coefficient of $g(x)$ is b_1 and the leading coefficient of $h(x)$ is b_2 then $b_1 b_2 = b$ and A and B are rational numbers with denominators dividing b_1 and b_2 respectively. Also, by Lemma 3.3 if $p \mid a$ then $p \mid A$ and $p \mid B$ and if $p \parallel b$ or $p \parallel c$ then p divides at least one of A, B. Therefore, $bAB \in \mathbb{Z}$ and it is divisible by $(\prod_{p|a} p)^2 (\prod_{p\|b} p)(\prod_{p\|c} p)$. On the other

hand, by Lemma 2.6 if $a \gg 1$ then

$$|A| \le \deg(g) \cdot (1 + \max(|x_i|)) \le \left(2 + \frac{\varepsilon}{5}\right) \deg(g).$$

The same is true for h. Because $\deg(g)$ and $\deg(h)$ are both less than a,

$$bAB < \left(2 + \frac{\varepsilon}{5}\right)^2 a^2 b < (4 + \varepsilon) a^2 b.$$

The condition (1) now implies that $AB = 0$. We may and will assume that $A = 0$. To complete the proof of the theorem we first prove the following proposition which says that if $A = 0$ then $\deg(g)$ is small.

PROPOSITION 3.1. *In the above notation, if $A = 0$ then for $a \gg 1$,*

$$\deg(g) < 28\sqrt{a \ln a}.$$

P r o o f. The basic idea is that the roots x_i of $f_{abc}(x)$ are somewhat uniformly distributed around the unit circle so $\mathrm{Re}(1 - x_i)$ is almost always positive and when it is negative it is rather small in absolute value. To be more precise, Lemma 2.6 implies that for a large enough,

$$r_i < 1 + \frac{3 \ln a}{a}, \quad \text{where } \; x_i = r_i e^{\varphi_i}, \; -\pi < \varphi_i \le \pi.$$

Therefore $\mathrm{Re}(1 - x_i) > -3(\ln a)/a$. Also, it follows that if $|\varphi_i| > 4\sqrt{\ln a}/\sqrt{a}$ then for $a \gg 1$,

$$\cos \varphi_i < \left(1 - \frac{7 \ln a}{a}\right).$$

In this case

$$\mathrm{Re}(1 - x_i) = 1 - r_i \cos \varphi_i > 1 - \left(1 + \frac{3 \ln a}{a}\right)\left(1 - \frac{7 \ln a}{a}\right).$$

This is greater than $3(\ln a)/a$ for $a \gg 1$.

By Theorem 2.1 the number of roots of $f_{abc}(x)$ with $|\varphi_i| \le 4\sqrt{\ln a}/\sqrt{a}$ is bounded by

$$\frac{8\sqrt{\ln a}}{2\pi\sqrt{a}} n + 12\sqrt{n \ln(n+1)} < 14\sqrt{a \ln a}.$$

So if $\deg g(x) \ge 28\sqrt{a \ln a}$ then for more than half of the roots of $g(x)$ we have $|\varphi_i| > 4\sqrt{\ln a}/\sqrt{a}$ and by the above calculations $A = \mathrm{Re}(A)$ is positive. As we assumed that $A = 0$, the proposition is proven.

So, it is enough to show that $f_{abc}(x)$ cannot have divisors of small degree. First of all, for $a \gg 1$, $g(x)$ must be monic by Lemma 3.2(2). Then if its constant term is not ± 1 at least one of its roots has absolute value of at least $2^{1/\deg g}$. And if its constant term is ± 1 Lemma 2.2(3) allows us to apply Smyth's result [18] to conclude that one of its roots has absolute value of at

least $\beta^{1/\deg g}$, where $\beta^3-\beta-1=0$. For $a\gg 1$ this is impossible by Lemma 2.6, so the theorem is proven.

Remark 3.8. Instead of using Smyth's result one can give a self-contained proof of the above theorem by showing that the sums of $(1-x_i)x_i^l$ over the roots of $g(x)$ are zeros for $1\le l\le \deg g$ (cf. [3]).

Remark 3.9. The constant $4+\varepsilon$ in the above theorem can be improved to $2+\varepsilon$ by noticing that $\deg(g)+\deg(h)=a-2$ and that A and B cannot be too negative as a corollary of Theorem 2.1. One can also make the $a\gg 1$ condition above explicit, for any fixed ε.

Theorem 3.9. *The number of coprime triples $a=b+c$, $b<c$, with $a\le A$ which satisfy*

$$\Big(\prod_{p\mid a}p\Big)^2\Big(\prod_{p\| b}p\Big)\Big(\prod_{p\| c}p\Big)\ll a^2b \tag{2}$$

is bounded by $CA^{20/11}\ln A$ where C is some constant independent of A.

Proof. Decompose $a=a_1a_2^2$, where a_1 is square-free. Then $\prod_{p\mid a}p\ge a_1$. Also, we can decompose (not uniquely) $b=b_1b_2^2b_3^3$ and $c=c_1c_2^2c_3^3$, where $b_1=\prod_{p\| b}p$ and $c_1=\prod_{p\| c}p$. Then

$$a^2bc=a_1^2a_2^4b_1b_2^2b_3^3c_1c_2^2c_3^3$$

and because $a_1^2b_1c_1\ll a^2b$ by (2), we get

$$a_2^4b_2^2b_3^3c_2^2c_3^3\gg c\gg a.$$

It follows that either $a_2b_2\gg a^{2/11}$, $a_2c_2\gg a^{2/11}$, or $b_3c_3\gg a^{1/11}$. The argument for the first two situations is similar, so we only give the argument when $a_2b_2\gg a^{2/11}$ and $b_3c_3\gg a^{1/11}$. Suppose first that $a_2b_2\gg a^{2/11}$. Then the number of triples (a,b,c) with $a=b+c$ is bounded by

$$\begin{aligned}\sum_{1\le a_2\le A^{1/2}}&\#\{a\in[1,A]:a_2^2\mid a\}\sum_{1\le b_2\le A^{1/2}}\#\{b\in[1,A]:b_2^2\mid b,\ b\ll(a_2b_2)^{11/2}\}\\&\ll\sum_{1\le a_2\le A^{1/2}}\frac{A}{a_2^2}\Bigg(\sum_{1\le b_2\le A^{2/11}/a_2}\frac{(a_2b_2)^{11/2}}{b_2^2}+\sum_{A^{2/11}/a_2<b_2\le A^{1/2}}\frac{A}{b_2^2}\Bigg)\\&\ll\sum_{1\le a_2\le A^{1/2}}\frac{A}{a_2^2}A^{1-2/11}a_2\ll\sum_{1\le a_2\le A^{1/2}}\frac{A^{2-2/11}}{a_2}\ll A^{20/11}\ln A.\end{aligned}$$

For $b_3c_3\gg a^{1/11}$ the number of triples (a,b,c) with $a=b+c$ is bounded by

$$\sum_{1\le b_3\le A^{1/3}}\#\{b\in[1,A]:b_3^3\mid b\}\sum_{1\le c_3\le A^{1/3}}\#\{c\in[1,A]:c_3^3\mid c,\ c\ll(b_3c_3)^{11}\}$$

$$\ll \sum_{1\le b_3\le A^{1/3}} \frac{A}{b_3^3}\Bigg(\sum_{1\le c_3\le A^{1/11}/b_3} \frac{(b_3c_3)^{11}}{b_3^3} + \sum_{A^{1/11}/b_3<c_3\le A^{1/3}} \frac{A}{b_3^3}\Bigg)$$

$$\ll \sum_{1\le b_3\le A^{1/3}} \frac{A}{b_3^3}A^{1-2/11}b_3^2 \ll \sum_{1\le b_3\le A^{1/3}} \frac{A^{2-2/11}}{b_3} \ll A^{20/11}\ln A.$$

Combining the above, we see that the number of coprime triples (a,b,c) as in the theorem is $O(A^{20/11}\ln A)$.

COROLLARY 3.1. *The set of coprime triples where $f_{abc}(x)$ is reducible has density zero in the set of all coprime triples.*

P r o o f. This follows from Theorems 3.8 and 3.9 and the well-known fact that the number of coprime pairs (a,b) where $a>b$ with $a\le A$ is asymptotically equivalent to $\frac{6}{\pi^2}\cdot\frac{A^2}{2}$. According to Donald Knuth (cf. [7], p. 324) this fact is due to L. Dirichlet.

Now we consider what happens if one fixes b. When $b=2$ then $f_{abc}(x)$ is always irreducible by Theorem 3.4. Also, Theorem 3.5 gives a partial result for b being an odd prime. The following theorem (with the corollary after it) shows that for any fixed b the *abc*-polynomial is irreducible for the set of a's having density one. In the following theorem and its corollary some of the implied constants in $\gg$ and $\ll$ depend on b.

THEOREM 3.10. *If b is fixed, then the number of coprime triples $a=b+c$ with $a<A$ and*

$$\Big(\prod_{p\mid a} p\Big)^2\Big(\prod_{p\| c} p\Big) \ll a^2 \tag{3}$$

is at most $C(b)A^{13/15}$, where $C(b)$ is some constant depending on b.

P r o o f. As in Theorem 3.9, decompose $a=a_1a_2^2$ and $c=c_1c_2^2c_3^3$. Because $a^2c=a_1^2a_2^4c_1c_2^2c_3^3$ and (3) implies that $a_1^2c_1\ll a^2$, we get

$$a_2^4c_2^2c_3^3 \gg c \gg a.$$

It follows that either $a_2\gg a^{2/15}$, $c_2\gg a^{2/15}$, or $c_3\gg a^{1/15}$. The argument for the first two situations is similar so we only give the argument when $a_2\gg a^{2/15}$ and $c_3\gg a^{1/15}$. Suppose first that $a_2\gg a^{2/15}$. Then the number of triples (a,b,c) with $a=b+c$ is bounded by

$$\sum_{1\le a_2\le A} \#\{a : a_2^2\,|\,a,\ a\ll a_2^{15/2},\ a\le A\}$$

$$\ll \sum_{1\le a_2\le A^{2/15}} \left(\frac{a_2^{15/2}}{a_2^2}\right) + \sum_{A^{2/15}\le a_2\le A} \left(\frac{A}{a_2^2}\right) \ll A^{13/15}.$$

For $c_3 \gg a^{1/15}$ the number of triples (a,b,c) with $a=b+c$ is bounded by

$$\sum_{1\le c_3\le A} \#\{c : c_3^3 \mid c,\ c \ll c_3^{1/5},\ c\le A\}$$
$$\ll \sum_{1\le c_3\le A^{1/15}} c_3^{12} + \sum_{A^{1/15}\le c_3\le A} \left(\frac{A}{c_3^3}\right) \ll A^{13/15}.$$

Combining all the estimates gives the theorem.

COROLLARY 3.2. *For any fixed b, $f_{abc}(x)$ is irreducible for a set of natural numbers a coprime to b having density one.*

Proof. This follows from Theorems 3.8 and 3.10 and a trivial observation that $\#\{a : a<A,\ \gcd(a,b)=1\} \gg A$.

If b is good in the sense that there is a prime p which divides it in exactly the first power, then the following theorem proves that all but finitely many abc-polynomials are irreducible. It also provides a rather small bound for the possible exceptions. Note that almost all (in the sense of density) b's are good in the above sense.

THEOREM 3.11. *Suppose p is a prime, $p \parallel b$. Suppose also that $c \ge b\max(\kappa, \log_2 b)$, where $\kappa = 11.21685874\ldots$ is such that $\beta^\kappa = 1+2\kappa$, where $\beta^3-\beta-1=0$. Then $f_{abc}(x)$ is irreducible.*

Proof. Suppose $f_{abc}(x) = g(x)h(x)$. Then as in Lemma 3.2 one of the polynomials $g(x)$, $h(x)$ has none of the c roots x_i of $f_{abc}(x)$ with $v_p(x_i)<0$. We may assume this is $g(x)$. Then $\deg g(x) \le b-2$. By our assumption $\deg g \le b-2 < b < c/\log_2 b$, so by Lemma 3.2(2), $g(x)$ is monic. If its constant term is not ± 1 then at least one of its roots has absolute value of at least $2^{1/d}$, where $d=\deg(g)$. If its constant term is ± 1, by Lemma 2.2(3) one can still conclude that one of its roots has absolute value of at least $\beta^{1/d}$ with β as above, by applying Smyth's result on the Lehmer's conjecture (cf. [18]).

As a result, we get a root x of $g(x)$ and therefore of $f_{abc}(x)$ with $|x| \ge \beta^{1/d} > \beta^{1/b}$. But by the estimate in the proof of Lemma 2.5,

$$|x| \le \left(1+\frac{2c}{b}\right)^{1/c}.$$

Combining the above, we get

$$\beta^{c/b} < \left(1+\frac{2c}{b}\right).$$

Therefore for κ as in the theorem, $c/b<\kappa$. The theorem follows.

4. Miscellanea and heuristics. First of all, combining the results of Section 3 one can easily check that $f_{abc}(x)$ is always irreducible for all $a \leq 24$ except for $f_{9,5,4}$ (and $f_{9,4,5}$, of course) and $f_{16,15,1}$. It is a simple exercise to verify their irreducibility separately by the same methods (cf. [3]) or one can just check it, say, with Maple. By the way, Maple can be used to verify the irreducibility up to a couple of hundreds. I do not know if the irreducibility is related in any way to the *abc* conjecture. The main Theorem 3.8 is about the triples which are not interesting from the point of view of the *abc* conjecture. However, Theorems 3.11 and 3.1 do include some interesting triples.

Let us now discuss a little the hypothetical approaches to the *abc* conjecture using the *abc*-polynomials. The first idea would be to try something similar to the geometric case, i.e. to construct a second polynomial, $g_{abc}(x)$, such that (f, g) is globally bounded but locally big. By this I mean that it has to be on the one hand divisible by a (large) power of any p dividing abc and, on the other hand, be bounded by some inequalities on the complex plane. The main problem is to capture the rather subtle dependence of the distribution of the roots of $f_{abc}(x)$ inside the clusters upon k (in the notation of Lemmas 2.8–2.11) without making the degree or coefficients of $g(x)$ too large.

Two other things one can try are the following.

1. One can try to study Arakelov geometry of some curves related to $f_{abc}(x)$, e.g. the hyperelliptic curve $y^2 = f_{abc}(x)$ over $\mathbb{Q}$, and the elliptic curve $y^2 = x(x-1)(x-\lambda)$ over the *abc*-field, where $f_{abc}(\lambda) = 0$. As far as hyperelliptic curves are concerned there is a recent result of I. Kausz (cf. [6]) on ω^2 of semistable hyperelliptic curves. Although $y^2 = f_{abc}(x)$ is not a semistable model its fibers are under control. A more serious problem is that its genus depends on a and Kausz's estimates "at infinity" depend heavily on the genus as they involve a choice of a metric on the relative dualizing sheaf of the universal stable curve of given genus.

2. Modulo the irreducibility conjecture, one can try to investigate some invariants of *abc*-fields, like Galois group, regulator, or ζ-function. One thing which is quite obvious is that there are lots of *abc*-units hanging around. (By *abc*-units I mean elements of the *abc*-field which have zero valuations for all primes not dividing *abc*.) Namely, x, $x^a - 1$, $x^b - 1$, $x^c - 1$ and all divisors of the last three polynomials evaluated at the root of *abc*-polynomial are *abc*-units. For instance, we have a lot of solutions of the equation $x + y = 1$ in *abc*-units. The theory of S-units and S-unit equations is well developed (cf., e.g., [2], [5], [15]). I do not know, however, if it is better to apply the theory to the roots of $f_{abc}(x)$ instead of just to $b/a + c/a = 1$.

References

[1] Yu. F. Belotserkovskiĭ, *Uniform distribution of algebraic numbers near the unit circle*, Vestsi Akad. Navuk BSSR Ser. Fiz. Mat. Navuk 1988 (1), 49–52 (in Russian).

[2] F. Beukers and H. P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*, Acta Arith. 78 (1996), 189–199.

[3] A. Borisov, *On some polynomials, allegedly related to the abc conjecture*, 1997, http://www.math.uiuc.edu/Algebraic-Number-Theory/.

[4] P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. 51 (1950), 105–119.

[5] J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications*, in: New Advances in Transcendence Theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, 110–174.

[6] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, IHES, preprint, 1996.

[7] D. Knuth, *The Art of Computer Programming*, Vol. 2, 2nd ed., 1981.

[8] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, 2nd ed., Grad. Texts in Math. 58, Springer, New York, 1984.

[9] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematika 7 (1960), 98–100.

[10] —, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), 257–262.

[11] R. C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecture Note Ser. 96, Cambridge Univ. Press, Cambridge, 1984.

[12] J.-L. Nicolas et A. Schinzel, *Localisation des zéros de polynômes intervenant en théorie du signal*, in: Lecture Notes in Math. 1415, Springer, Berlin, 1990, 167–179.

[13] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki, Vol. 1987/88, Exp. 694, Astérisque 161–162 (1988), 165–186.

[14] A. Schinzel, *Reducibility of lacunary polynomials. IX*, in: New Advances in Transcendence Theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, 313–336.

[15] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. 1467, Springer, Berlin, 1991.

[16] E. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. 4 (1956), 287–302.

[17] J. H. Silverman, *The S-unit equation over function fields*, Math. Proc. Cambridge Philos. Soc. 95 (1984), 3–4.

[18] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.

[19] W. W. Stothers, *Polynomial identities and Hauptmoduln*, Quart. J. Math. Oxford Ser. (2) 32 (1981), 349–370.

Department of Mathematics
The Pennsylvania State University
University Park, Pennsylvania 16802
U.S.A.
E-mail: borisov@math.psu.edu

Received on 2.12.1996
and in revised form on 30.10.1997 (3090)